NIAP Review Briefing To

Information Security and Privacy Advisory Board
03/17/04; 1515; Hyatt Regency
Dr. Gregory N Larsen; IDA
703-845-6661; glarsen@ida.org

Background

- Page-47; National Strategy to Secure Cyberspace
  - Additionally, the federal government will be conducting a comprehensive review of the National Information Assurance partnership (NIAP), to determine the extent to which it is adequately addressing the continuing problem of security flaws in commercial software products. This review will include lessons learned from implementation of the Defense Department's July 2002 policy requiring the acquisition of products reviewed under the NIAP or similar evaluation processes.
- Paraphrasing…
  - Make a business case for a NIAP process…

2

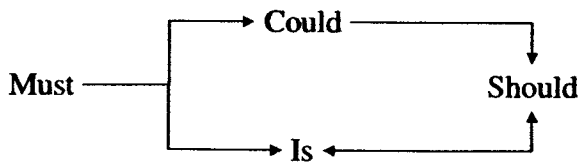
Background

- National Strategy to Secure Cyberspace
  - …comprehensive review of NIAP…
- "Comprehensive", example questions from Stakeholders
  - Are Protection Profiles (PP) adequate? [complete, accurate, useable]
  - Is the Review process adequate? [complete, accurate, meet expectations]
  - Is the cost worth the return? […and who bears the cost?]
  - Are sufficient products NIAP evaluated and listed? [or in "evaluation"]
  - Are results of evaluations used in acquisitions/by users? In SAA for C&A? to build architectures?
  - What are the trends for vendors to have products evaluated? [or is this mostly marketing to the vendor?]
  - Does the current process present conflicts-of-interests? [money, quality, monoply issues]
  - Etc.

3

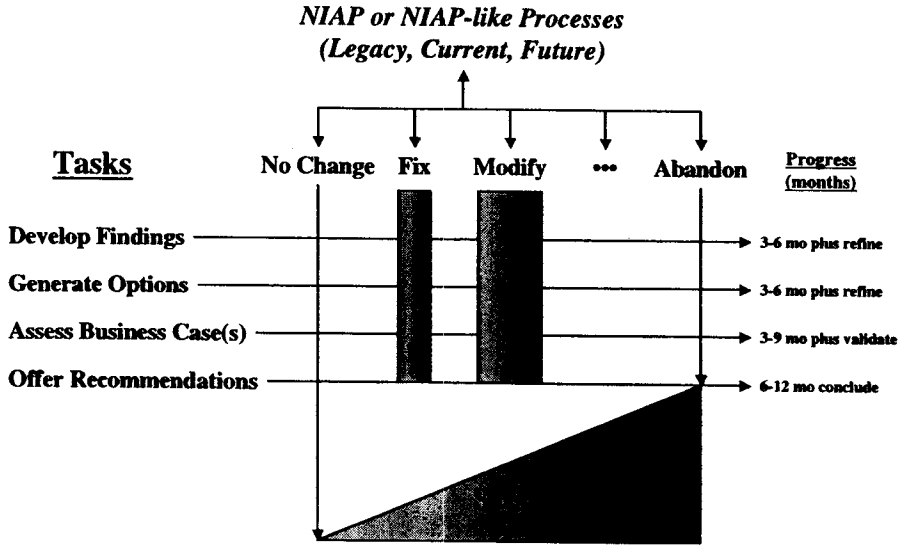
General Approach

- Develop the facts, information, arguments, and recommendations concerning:
  - What must NIAP be? (National policy threshold)
  - What is NIAP? (Experience and fact-finding)
  - What could NIAP be? (Expectation and situation)
  - What should NIAP be? (Analysis and Recommendations)



4

General Approach



5

Four Major Tasks

- Objective: Review the efficacy and affordability of NIAP capabilities and infrastructure
  - Characterize National intent, NIAP implementation, and stakeholder expectations, Conduct Fact finding, and Develop Issues
  - Assess impacts of selected issues and generate alternatives and options to address these issues
  - Analyze selected issues/options
  - Provide recommendations

6

General Task Framework

Task	Purpose	Intent	Experience	Output
Develop Starting Basis	Characterize	Original Purpose Future Needs	Barriers Limitations Discrepancies	**Findings** Issues Problems Expectations
Generate Options	Targets of Change	Remove/Reduce Improve/Increase Keep/Adjust	Pros/Cons	**Options** No Change Fix Modify Abandon Eliminate Limit
Assess Business Case of Options	Feasibility of Change	Proposed Price and Performance	Current Costs and Capabilities	**Business Case** P/P Operating Point Strategy to next Operating Point
Recommend Actions	Policy, Program, Resource Mix	Future Basis	Current Basis	**Recommendations** Justify | Near-term Exploit | Mid-term Rectify | Long-term Abandon

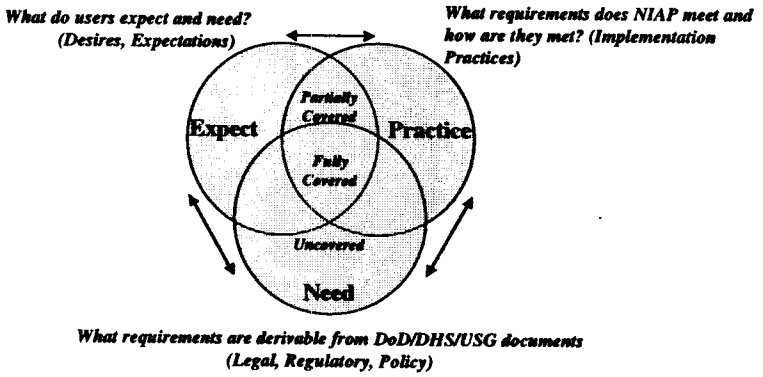
7

Stage 1: Current Activity

- Generate independent descriptions of "requirements"
  - Legal, statutory, policy "requirements" analysis (must)
  - Experiential "requirements" of NIAP process assessment (is)
  - Expectation "requirements" by interviews (could)
- Conduct workshop(s) (should)
  - Assess issues amenable to education and training
  - Develop changes feasible now
  - Document changes potentially feasible should specific conditions change
- Develop and analyze options and recommendations
- Report

8

Requirements Approach



9

Concept of a Well-formed Requirement

- Requirement is well-formed when the following are identified
  - Authority --> origin or delegated
  - Responsibility --> assigned or assumed
  - Accountability --> explicit or implicit
- Early collection and assessment results indicate variance among each requirement set/viewpoint.
  - Education, training and awareness may resolve some differences
  - Analysis will surface which differences are the result of constraints
    - Resources
    - Limits on…
    - Barriers to…
    - Missing attributes/clarity/overlap of a well-formed requirement's attributes
    - Mal-distribution of authorities, responsibilities, accountabilities

10

Overall Review Activity Flow

- Gathering and assessing documents
- Compiling stakeholders/POCs
- Developing requirements from national documents
- Scripting interviews
- Schedule interviews (2 person teams)
- Compile Interviews
- Invitations to workshop
- Re-interview selected
- Develop expected needs from interviews/workshop
- Develop baseline of actual from NIAP practices/documents
- Develop compilation and comparison of coverages
- Propose movement opportunities to gain coverage
- Cost each move (legal, funds, etc.)
- Develop timing for each move
- Construct roadmap of feasible and affordable changes
- Document currently infeasible but possible with other changes [legal, technical, etc.]

11

Status of Activities

- Collection of documented requirements and current practices approximately 75% complete
  - Data-model and data-base to support further analysis and continued refinement initiated
- Interview requests solicited with additional interviews to be added as time permits
  - Initial interview script/questions developed and under internal review
  - Application to internal expertise to refine and use as mailed survey/interview scheduled
- Exploring workshop dates to reconcile and identify options to address findings generated from collection and analysis of requirements sets
- Baseline Report structured and being incrementally developed in parallel with review collection and analysis activities

12

Known or Anecdotal Issues

- Sample from Experience/Expectations
  - Money on the wrong side of the problem?
  - Expect safe products?
  - What does safe mean?
  - Should international agreements drive our evaluations?
  - Lab certifications separate from personnel?
  - NSSTSP-11 adequate?
  - What does "evaluated" mean?
  - Is truth in advertising sufficient? Or is it safety?
  - Etc.

13

Sample Questions for Review

- On what basis should USG be judging NIAP's success or failure?
- Is NIAP oversight of laboratory testing cost-effective? Timely? Comprehensive?
- Does NIAP's mission to conduct CC-based IT product evaluation remain current or does it need to be modified?
- Is NIAP increasing security or consumer trust in product?
- What, if any, are the inherent risks of foreign owners of labs and/or foreign products receiving evaluations?
- How do we assist small business, who can not afford the NIAP process?

14

Sample Questions for Review

- To what extent is NIAP accomplishing its mission?
- To what extent is NIAP accomplishing what is needed?
- Can the NIAP assurance model satisfy stakeholders needs?
- Should NIAP become an independent organization? Private-sector run?
- Does NIAP need to be improved overhauled refocused to better meet its current or updated mission? How?
- What are the impediments to improve NIAP? Recommendations to response? Resource needs?
- Do NIAP partners that conduct evaluations provide the level of trust needed for classified systems? Unclassified systems? Private-sector and critical infrastructure systems?
- What has been learned about the NSTISSP#11 policy implementation in national security community? Does this support expanding the policy to cover USG unclassified systems?

15

Still in-work...

- How notionally will we package and report recommendations for change?
  - Overall report outlined and structured
  - Work product captured to this document and used as basis for final report construction
- What models of capability, cost, time, feasibility, impacts are we notionally using to assess, analyze, and evaluate the options and recommendations?
  - Notion of operational P/P or C/C movement as the basic business model
  - Ability to affect change (movement) is through policy, program, resource
  - Types of change (control, efficiencies, effectiveness)

16

NIAP Improvement

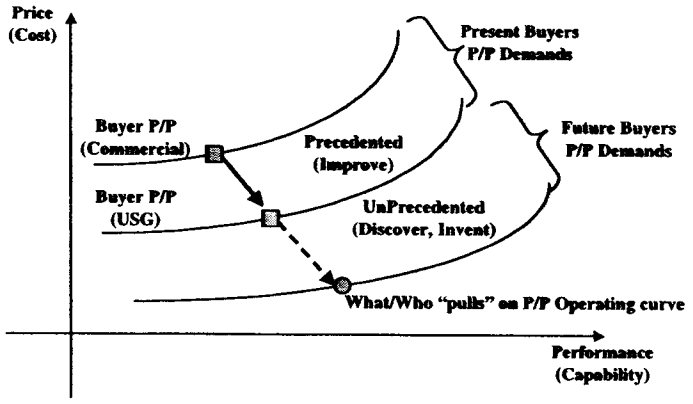
How will you satisfy priorities?

Change	Actions	Choice
Policy	List of possibilities	Selection of primary recommendation
Program	List of possibilities	Selection of primary recommendation
Resource	List of possibilities	Selection of primary recommendation

17

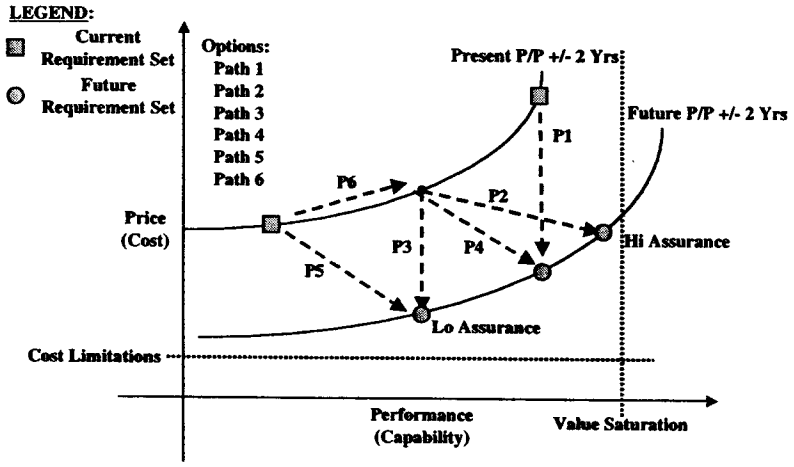
Notion-1

Where is NIAP operating today?



18

Movement Options

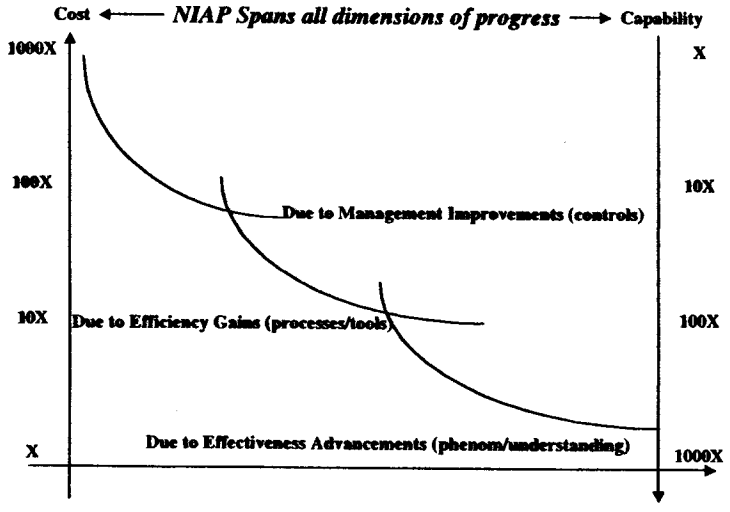


Feasibility:
What is feasible near-, mid-, long-term?
What set of requirements does a feasible set represent?
Where are the current requirement sets?

19

Notional "Package" Figure of Merit

Capability/Cost Ratio



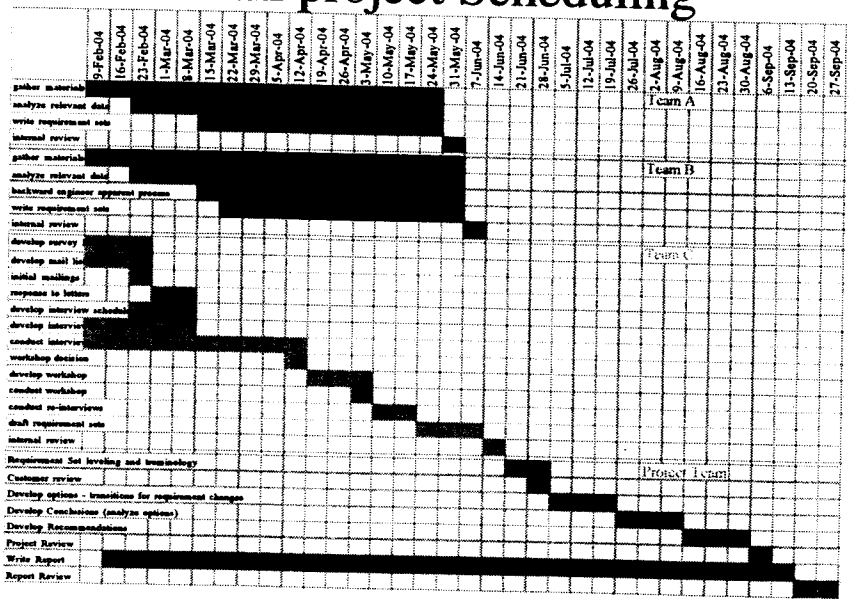
20

Notional Roadmap

2005	2010	2015	2020
Buy More "Stuff" better		Operate Better Focus: Buy sufficient assurance capabilities	
Engineering Practices Program		Empirical Focus: Best Practices Understanding 25% reduction in assurance variance through better controls over existing processes	
Technology Development Program		Process/Tools Focus: 50 % Improvement Decrease assurance variance to less than 25% for 90% of products	
Basic Research Program		Phenom/Understanding Focus: 200% assurance productivity Improvements Repeatedly engineer assurance intensive systems predicting assurance quality, performance, schedule and cost within 10%	

21

Overall project Scheduling



22